


Monterrey Chapter

# Planeación Estratégica de la Ciberseguridad

David Hernández, MBA

# ¿Qué es la PE?

La planeación estratégica es un proceso integral para determinar en qué debe convertirse una empresa y así como para determinar cuál es la mejor manera para lograr ese objetivo.

Evalúa todo el potencial de una empresa de manera explícita, y vincula los objetivos del negocio con las acciones y recursos requeridos para alcanzarlos.

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# ¿Cómo funciona la PE?

1. Describe la **misión, visión y los valores** fundamentales
2. Apunta a mercados potenciales explorando **oportunidades y amenazas**
3. Comprende las **prioridades** actuales y futuras de segmentos específicos
4. Analiza las **fortalezas y debilidades** en relación a los competidores
5. Define las expectativas de la partes interesadas y establece **objetivos claros y convincentes para el negocio**
6. Prepara programas, políticas y planes para **implementar la estrategia**
7. **Monitorea el desempeño** de la estrategia

Entre otros componentes

# Top 10 Management Tools

| 2006 | 2010 | 2012 | 2014 | 2017 |
|---|---|---|---|---|
| **1.** Strategic Planning | **1.** Benchmarking | **1.** Strategic Planning | **1.** CRM | **1.** Strategic Planning |
| **2.** CRM | **2.** Strategic Planning | **2.** CRM | **2.** Benchmarking | **2.** CRM |
| **3.** Customer Segmentation | **3.** Mission and Vision Statements | **3.** Employee Engagement Surveys | **3.** Employee Engagement Surveys | **3.** Benchmarking |
| **4.** Benchmarking | **4.** CRM | **4.** Benchmarking | **4.** Strategic Planning | **4.** Advanced Analytics |
| **5.** Mission and Vision Statements | **5.** Outsourcing | **5.** Balanced Scorecard | **5.** Outsourcing | **5.** Supply Chain Management |
| **6.** Core Competencies | **6.** Balanced Scorecard | **6.** Core Competencies | **6.** Balanced Scorecard | **6.** Customer Satisfaction |
| **7.** Outsourcing | **7.** Change Management | **7.** Outsourcing | **7.** Mission and Vision Statements | **7.** Change Management |
| **8.** Business Process Reengineering | **8.** Core Competencies | **8.** Change Management | **8.** Supply Chain Management | **8.** TQM |
| **9.** Scenario and Contingency Planning | **9.** Strategic Alliances | **9.** Supply Chain Management | **9.** Change Management | **9.** Digital Transformation |
| **10.** Knowledge Management | **10.** Customer Segmentation | **10.** Mission and Vision Statements | **10.** Customer Segmentation | **10.** Mission and Vision Statements |

BAIN & COMPANY

**How to use**: Rollover cells to see tool ranking trends. Click cells to see usage vs satisfaction.

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Porqué es importante la PEdC

- El foco en la ciberseguridad está en su punto más alto
  - ✓Incremento en el número de brechas
  - ✓Visibilidad a nivel de consejo y CEO

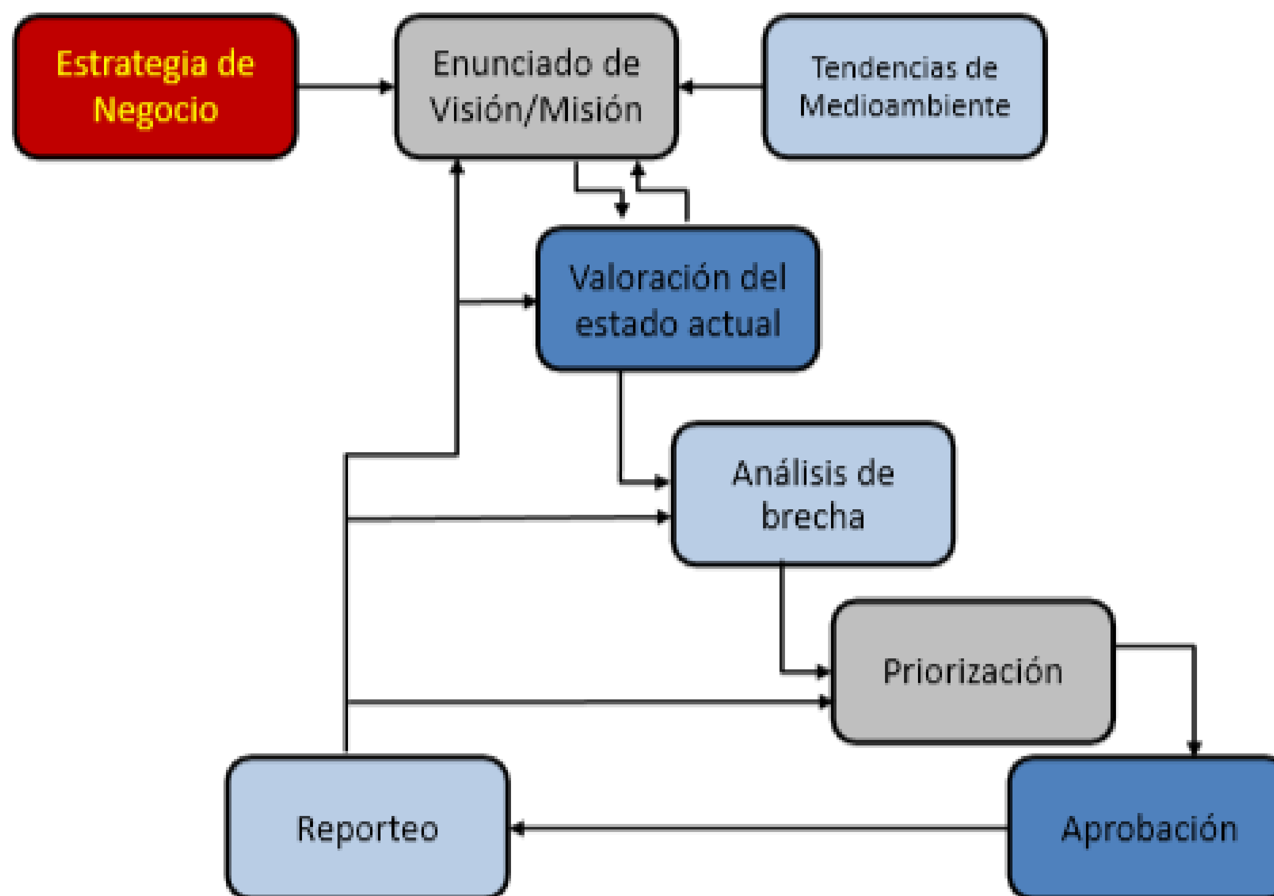
- Los equipos de Seguridad en la Información:
  - ✓Tienen más presupuesto (y opciones)
  - ✓Mayor responsabilidad y escrutinio

- Seguridad ya no es una preocupación de TI
  - ✓Es parte vital para el crecimiento del negocio
  - ✓Los llíderes de seguridad en las empresas tienen que aprender como navegar en este nuevo mundo

# Retos y áreas de oportunidad

1. El enfoque mayormente **técnico**
2. Una **desconexión** con las estrategia corporativa
3. Un **escaso análisis** del entorno de la organización
4. Una **omisión en las necesidades** de las partes interesadas
5. No contemplar los **resultados para el negocio**
6. Y esto cuando se realiza PEdC y **la operación** da un respiro…

# Proceso de la PEdC



ISACA®

Confianza en, y valor de los sistemas de información

Monterrey Chapter

# ¿Porqué entender el negocio?

- Muchos profesionales de seguridad no tienen un entendimiento de los objetivos del negocio
  - Desconexión entre seguridad y los líderes del negocio
  - Inhabilidad para identificar que proyectos de seguridad son importantes para el negocio.

# ¿Cómo lograrlo?

Averiguar por qué existe la empresa y qué está intentando lograr ➡ **visión y misión**

Entender necesidades de los líderes del negocio ➡ **partes interesadas (*stakeholders*)**

# Necesidades de las partes interesadas




Source: ISACA, COBIT 5, 2012

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# 1. Identificando (SIPOC)

| (S) Suppliers | (I) Inputs | (P) Process | (O) Outputs | (C) Customers |
|---|---|---|---|---|
| Business owner, Legal, Security. Regulations | Requeriments | Define requirements | Use case Project plans | Business owner<br>Technical teams<br>Project managers Finance, Comms |
| Business Operations team | Approved use cases<br>Approved project plans | Design | Technical architecture<br>Technical reqs | Engineering team<br>Security team<br>Operations team |
| Business owner, Legal, Security, Vendors, Technical | SLAs, Budget, Hardware & software reqs | Procure | Executed contacts | Business owner<br>Legal and Vendor |
| Vendors, Architects, Engineers | Technical reqs<br>System configuration | Build & Deploy | Migration plan running system | Business owner<br>Technical teams<br>Vendor, Leadersip Help Desk |
| Technical teams. Vendors | SLAs<br>Business uptime reqs | Manage the solution | Maintenance plan | Business owner Leadership (CEO, CFO, CIO, CISO) |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# 2. Mapeando

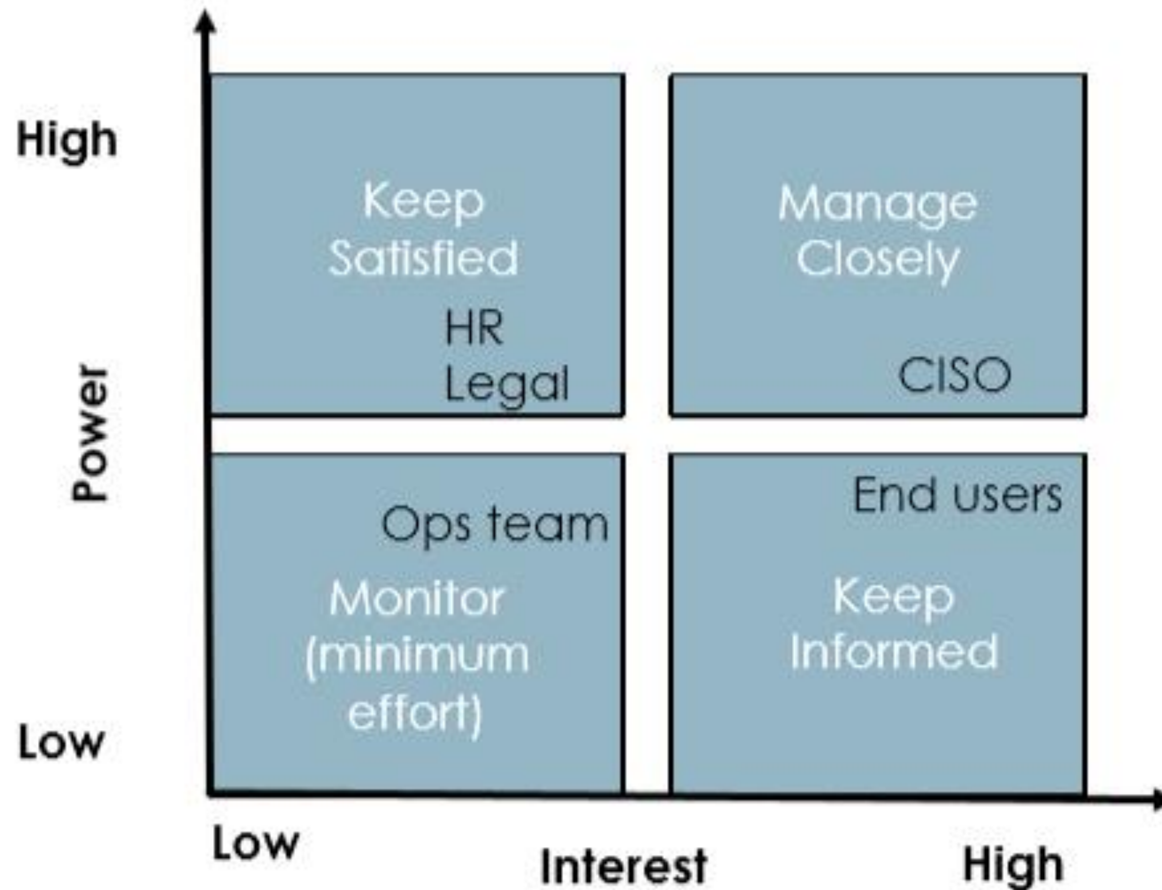
| Stakeholder | Power | Interest | Stakeholder Name | Views/Interest in project |
|---|---|---|---|---|
| CIO | Veto | High | | Innovation, risk, productivity |
| CFO | Veto | High | | Cost, risk |
| CISO | Vote | High | | Security, risk, compliance |
| HR | Vote | Medium | | Impact on employee polices |
| Legal | Vote | Medium | | Impact of laws, terms and conditions of contracts, eDiscovery |
| End Users | Voice | High | | Usability, Productivity |
| Ops Team | Voice | Low/Medium | | Project delivery time and budget |

ISACA®

Confianza en, y valor de los sistemas de información

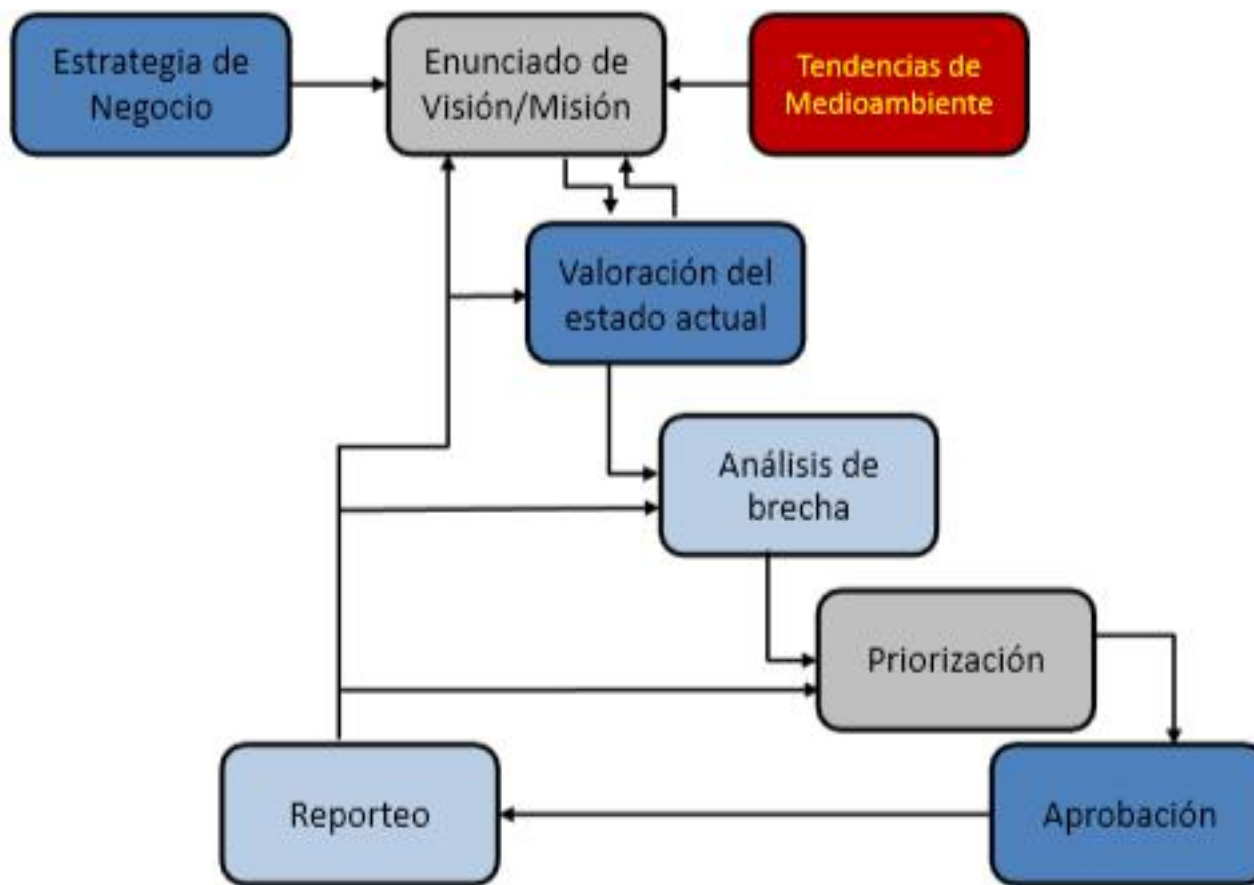
Monterrey Chapter

# 3. Priorizando



ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Proceso de la PEdC



ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Tendencias del entorno

- Comprender las preocupaciones de alto nivel de los principales líderes

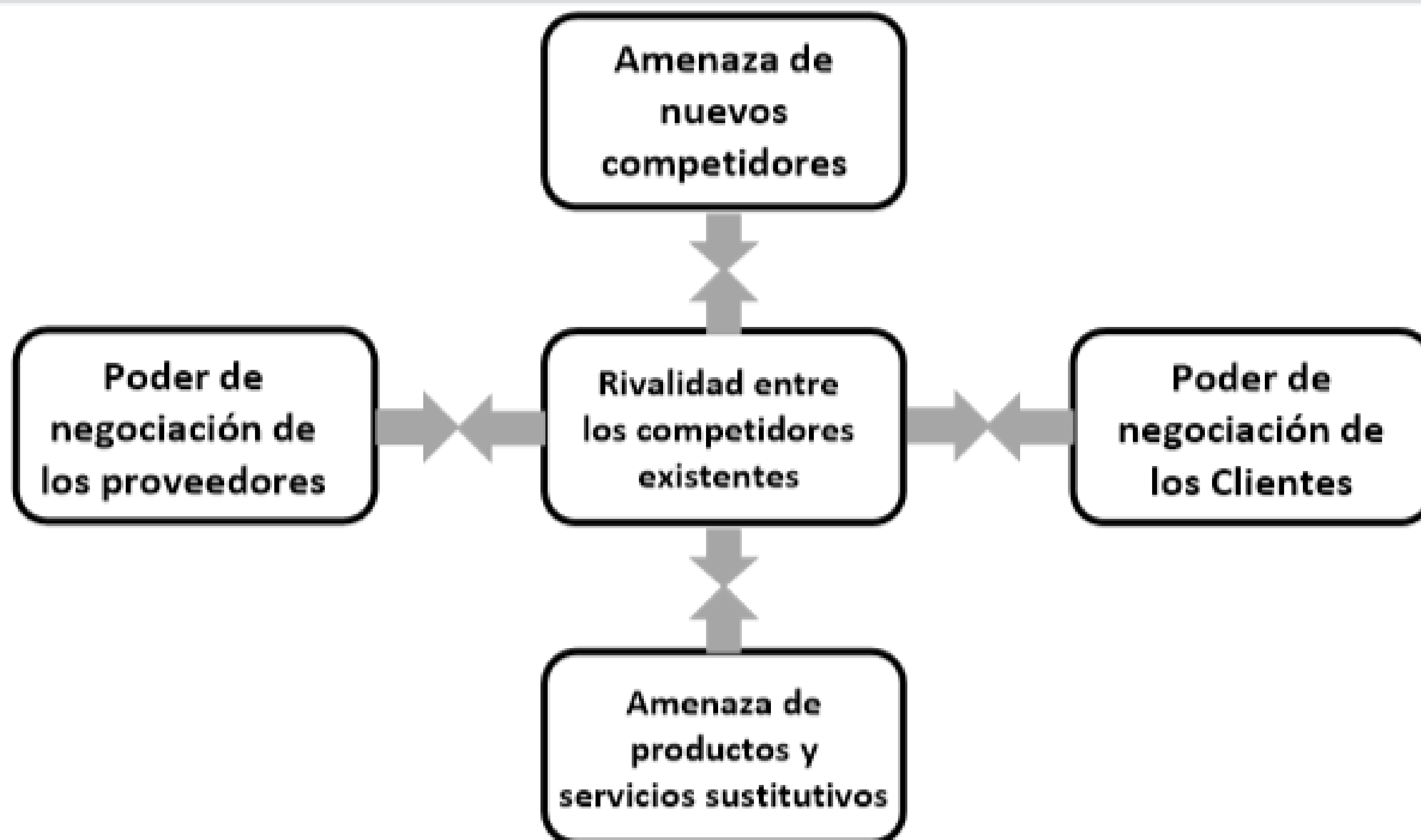
- Aprender cómo funciona la estrategia de negocios

# PEST

| Political | Economic |
|---|---|
| ▪ Regulations and restrictions related to international trade, tax policy and competition<br>▪ War, terrorism (e.g. 9/11 terrorist attack), outbreak of diseases (e.g. Ebola)- result in government intervention- likely to occur to protect passengers, interest and operation safety<br>▪ Airline industry consolidation (mergers and acquisitions) | • Cycle´s peaks and troughs<br>• Economic indicators<br>✓ U.S. economy is expanding through global production<br>✓ U.S. generating~200k jobs per month<br>✓ Real personal income is rising<br>✓ Household net worth is growing<br>▪ Fluctuation in oil prices-profitability<br>▪ Consumer confidence |
| **Social** | **Technological** |
| • Increased demand for air travel<br>• Younger generation travels more (Millennial generation expected to grow 50% by 2020 and remain strong for the next 15 años)<br>• Increased need for convenient travel options (upgrades, Wi-Fi, in-flight entertainment, refundable tickets, book through on-line travel agencies, mobile and travel apps | • Technology-adopt the latest to survive intense competition<br>• Advanced aircraft technology results in lower fuel consumption (30% of total operating expense) and address climate change (air travel is responsible for 12% of the total emissions from the transportation industry)<br>• IT solutions and mobile technology- connectivity and enhanced passenger experience |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# 5 fuerzas de Porter

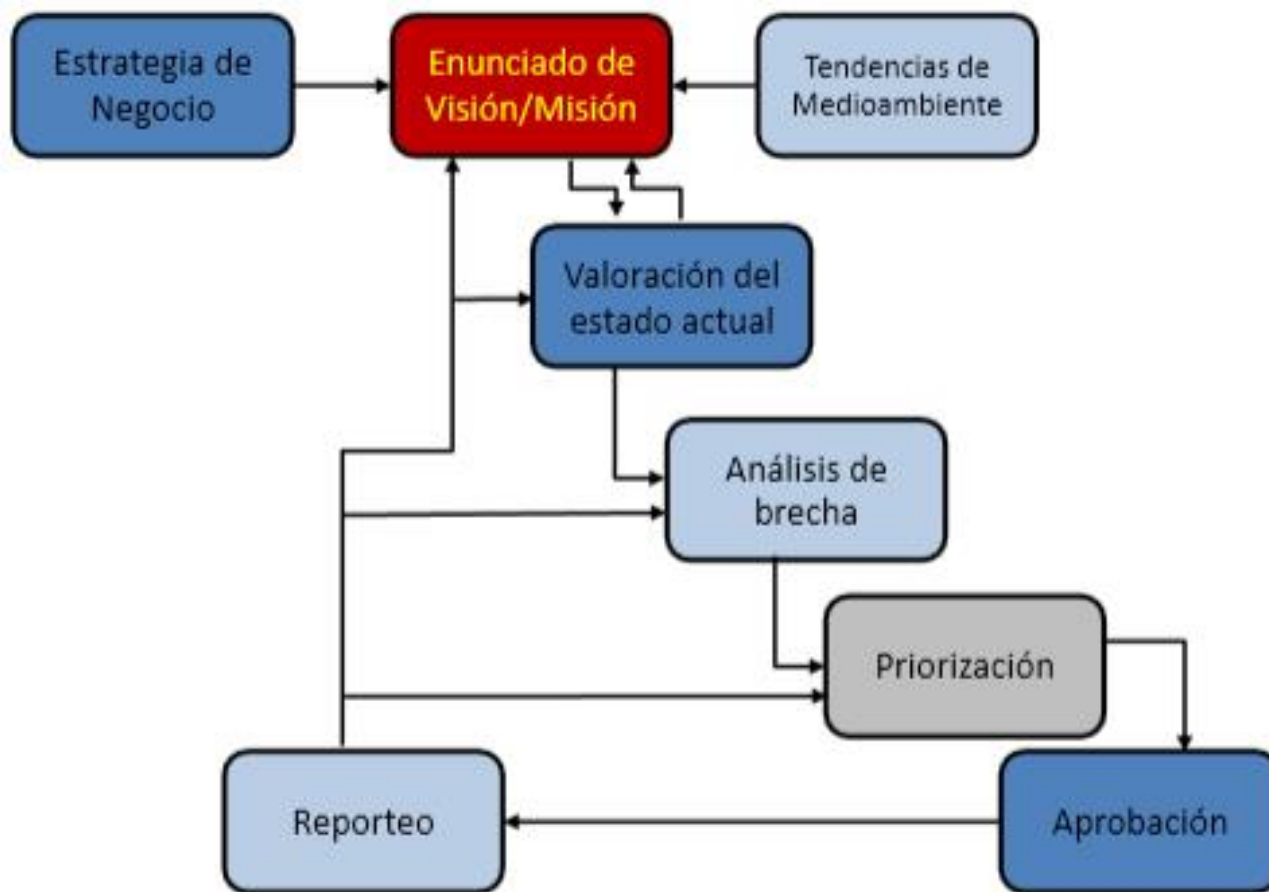


ISACA®

Confianza en, y valor de los sistemas de información

Monterrey Chapter

# Proceso de la PEdC



ISACA®

Confianza en, y valor de los sistemas de información

Monterrey Chapter

# Visión y Misión

**VISIÓN**

- ✓Representa el "por qué" de la organización
- ✓El noble propósito
- ✓El objetivo aparentemente inalcanzable

**MISIÓN**

- ✓Representa "qué" hace la organización hoy día
- ✓Describe qué somos y qué hacemos

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Creando la Misión

- Proteger a la empresa (evitar fallas
- Habilitar el negocio (asegurar el éxito)

***"Avanzar en la misión de la Compañía asegurando, defendiendo y monitoreando nuestros activos más importantes"***

# Visión de Seguridad

¿Cómo creamos valor para las partes interesadas?

¿Cómo innovamos?

¿Por qué nos necesitan?

- ¿Cuál es el problema que necesita ser resuelto?
- La aspiración que debe cumplirse

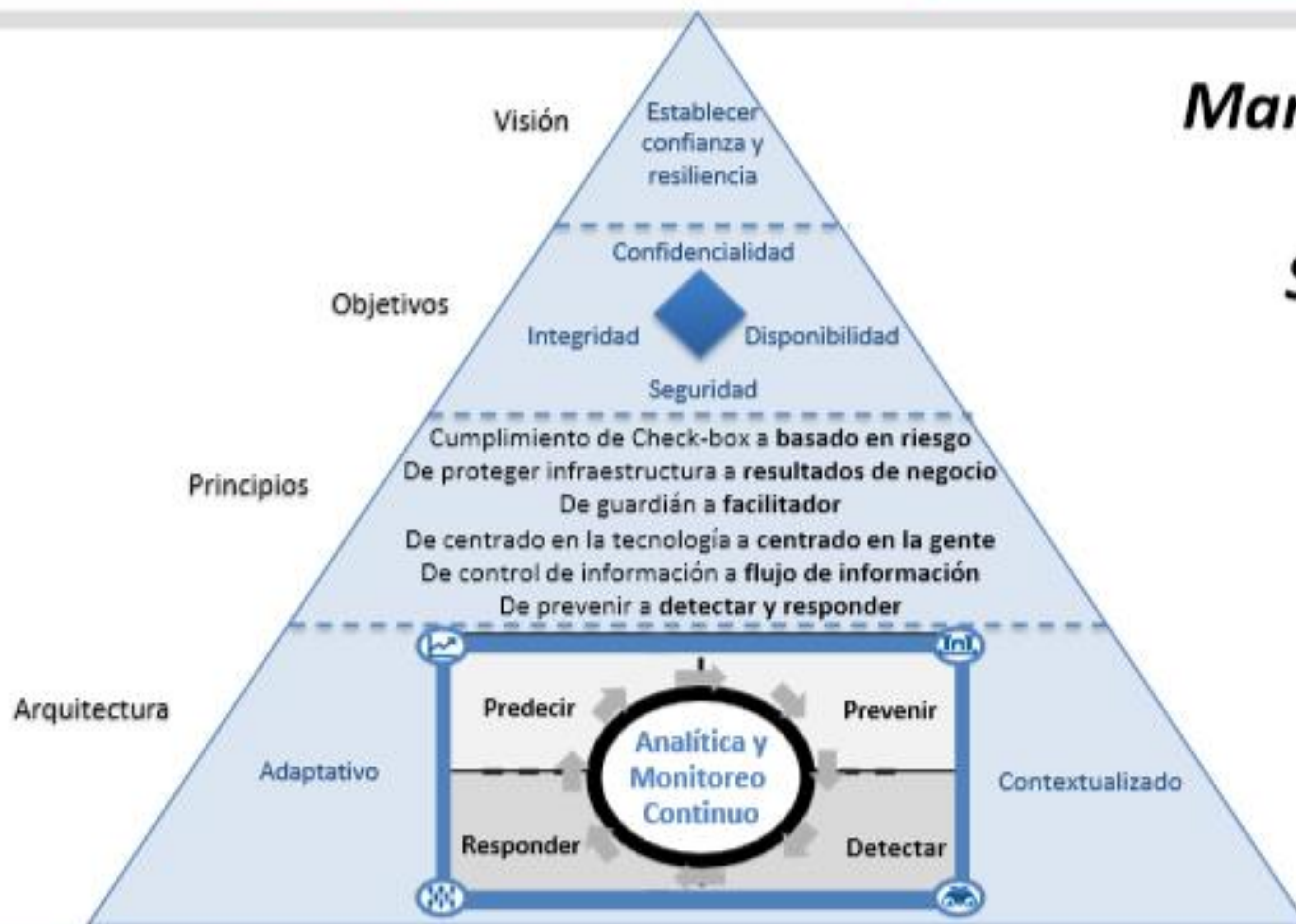
ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Marco de referencia

- Construir programas de seguridad
- La gestión del riesgo
- Comunicar a las partes interesadas

Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Visión de Seguridad

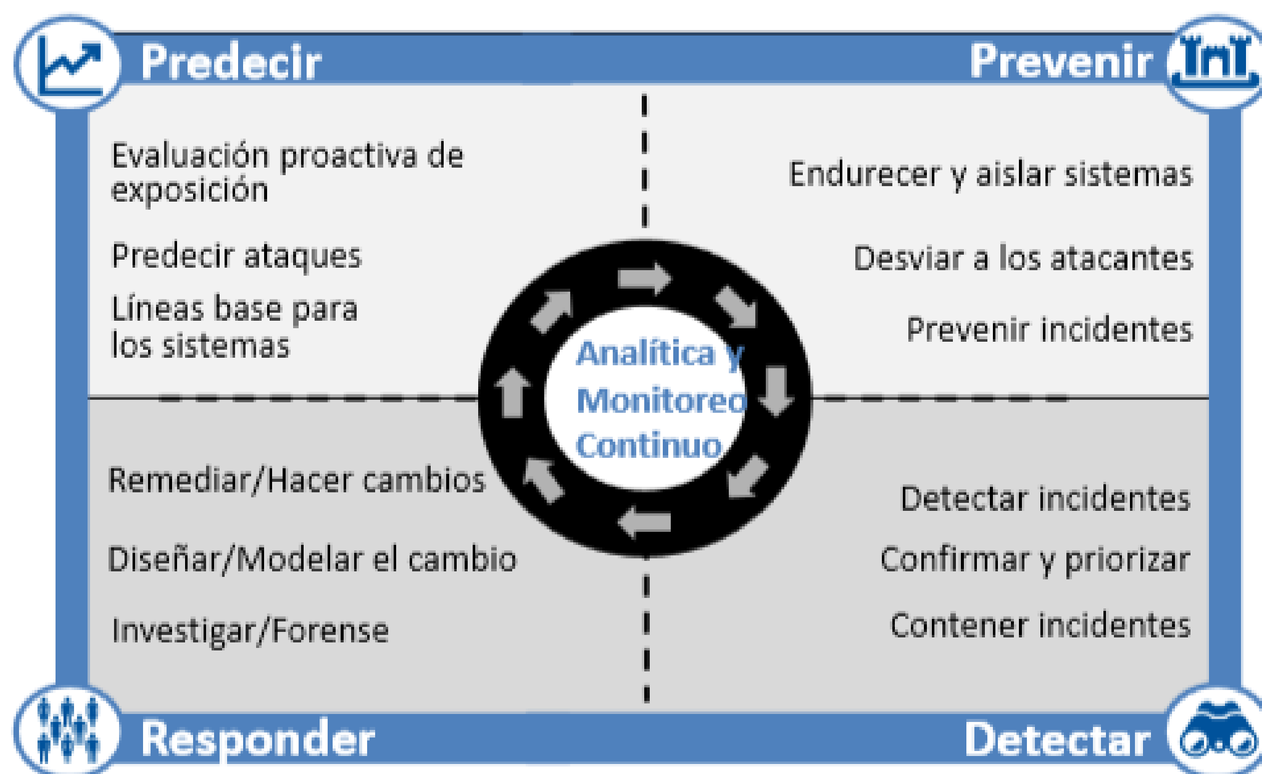



***Managing Risk and Security at the Speed of Digital Business***

"*Managing Risk and Security at the Speed of Digital Business*" Gartner, 2017

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Arquitectura de Seguridad Adaptativa




*"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"* Gartner, 2016

ISACA®

Confianza en, y valor de los sistemas de información

Monterrey Chapter

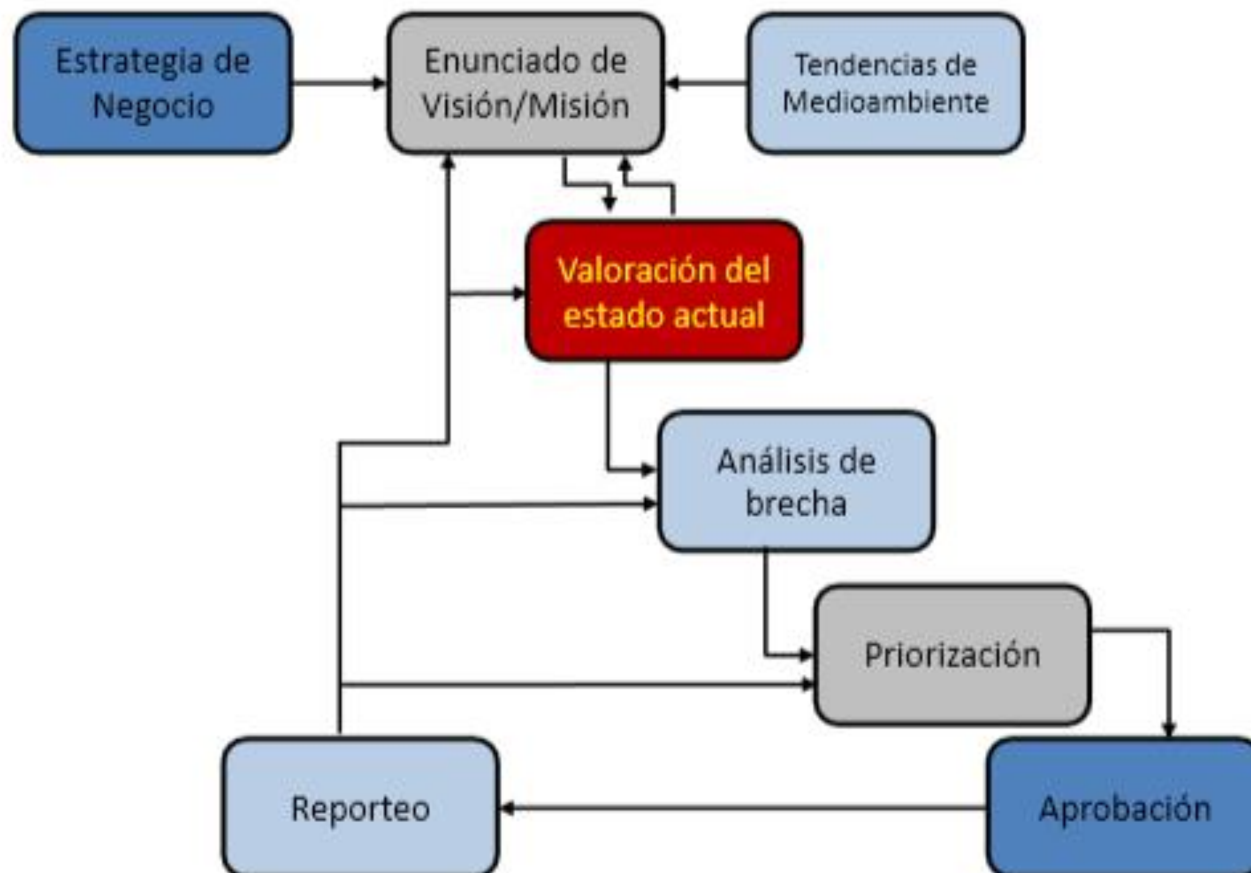
# NIST Cybersecurity Framework

| Function | Category |
|---|---|
| Identify | ▪ Asset Management<br>▪ Business Environment<br>▪ Governance<br>▪ Risk Assessment<br>▪ Risk Management Strategy |
| Protect | • Access Control<br>• Awareness & Training<br>• Data Security<br>• Information Protection Processes & Procedures<br>• Maintenance<br>• Protective Technology |
| Detect | ▪ Anomalies &Event<br>▪ Security Continuous Monitoring<br>▪ Detection Processes |
| Respond | ▪ Response Planning<br>▪ Communications<br>▪ Analysis<br>▪ Mitigation<br>▪ Improvements |
| Recover | ▪ Recovery Planning<br>▪ Improvements<br>▪ Communications |



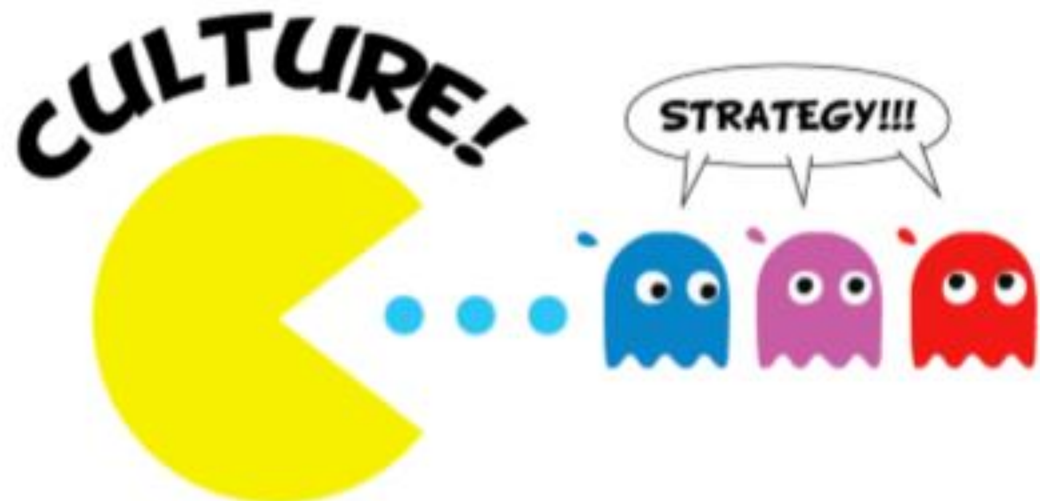

*"Framework for Improving Critical Infrastructure Cybersecurity"* NIST, 2014

# Proceso de la PEdC



# Estado Actual

1. Pruebas de penetración, valoración de riesgo y seguridad
2. Análisis histórico de la organización
3. Valores y Cultura
4. Análisis FODA



Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Analizando valores centrales

| Valores Centrales | ¿Cómo impacta este valor central mi equipo de seguridad? | ¿Cómo puede seguridad mostrar este valor central? |
|---|---|---|
| | | |
| | | |
| | | |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

## Análisis FODA

- Priorizar para obtener resultados exitosos
- Desarrollar un plan a corto y largo plazo
- Ganar y mantener una ventaja competitiva

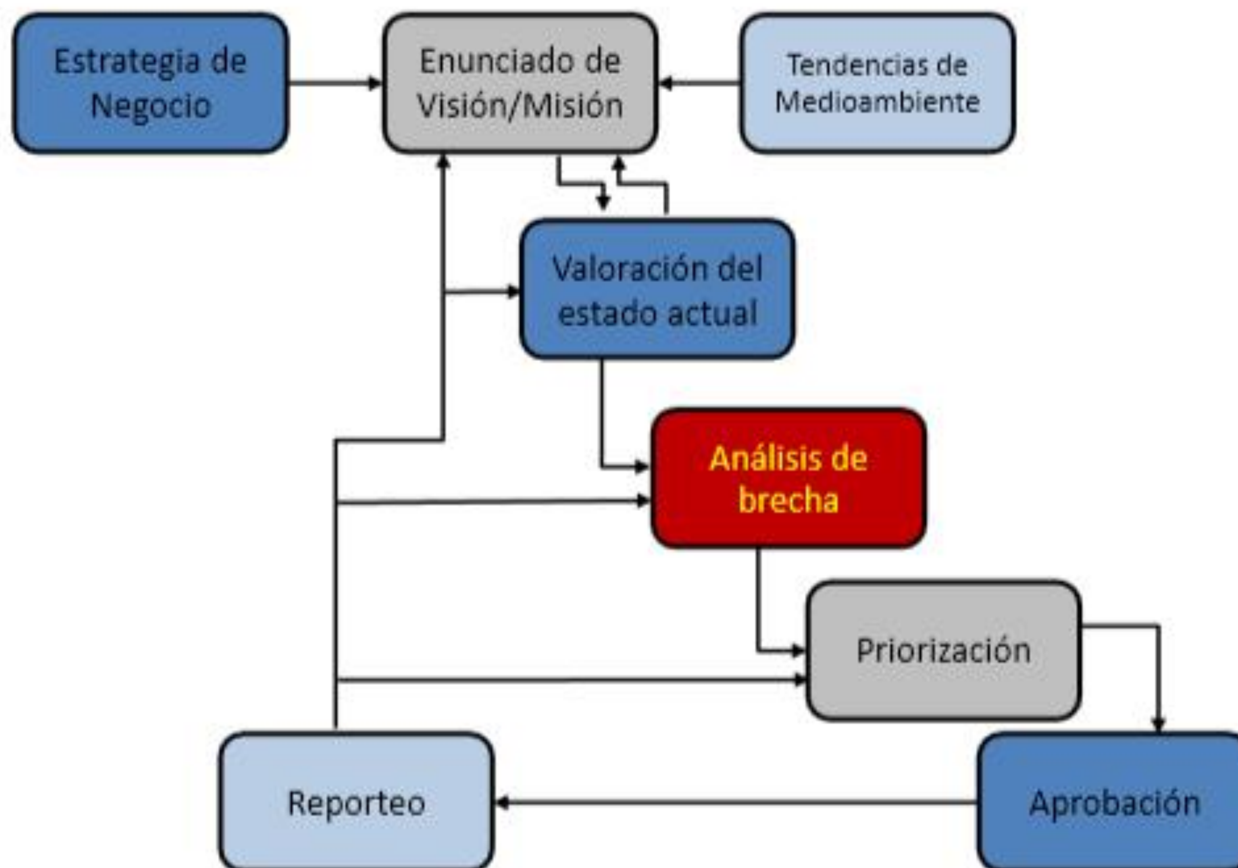
ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Análisis FODA

| | Ayudan | Perjudican |
|---|---|---|
| Interno | **Fortalezas** | **Debilidades** |
| Externo | **Oportunidades** | **Amenazas** |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Proceso de la PEdC



# Recordando el Análisis FODA

| | Helpful | Harmful |
|---|---|---|
| Internal | **Strengths**<br>• Business mission to help people lead healthier lives<br>• Culture of innovation and R&D<br>• Ability to create breakthrough new drugs<br>• Decentralized business units allow quick innovation<br>• Strong geographic presence<br>• Access to talent around the world | **Weaknesses**<br>• No CISO or central security responsibility<br>• Security is decentralized and understaffed<br>• No central threat strategy<br>• Technology is under utilized |
| External | **Opportunities**<br>• Hire a CISO<br>• Operationalize personnel to improve security effectiveness (combining physical & info sec)<br>• Leverage global presence to build 24x7 team<br>• Increase staffing levels | **Threats**<br>• Insider threat- geographically dispensed workface and risk or data loss<br>• Competitors-seeking intellectual property<br>• Nation state-seeking to accelerate R&D<br>• Regulatory-increased regulation results in delays getting new drugs to market |

# Estado Actual y Futuro

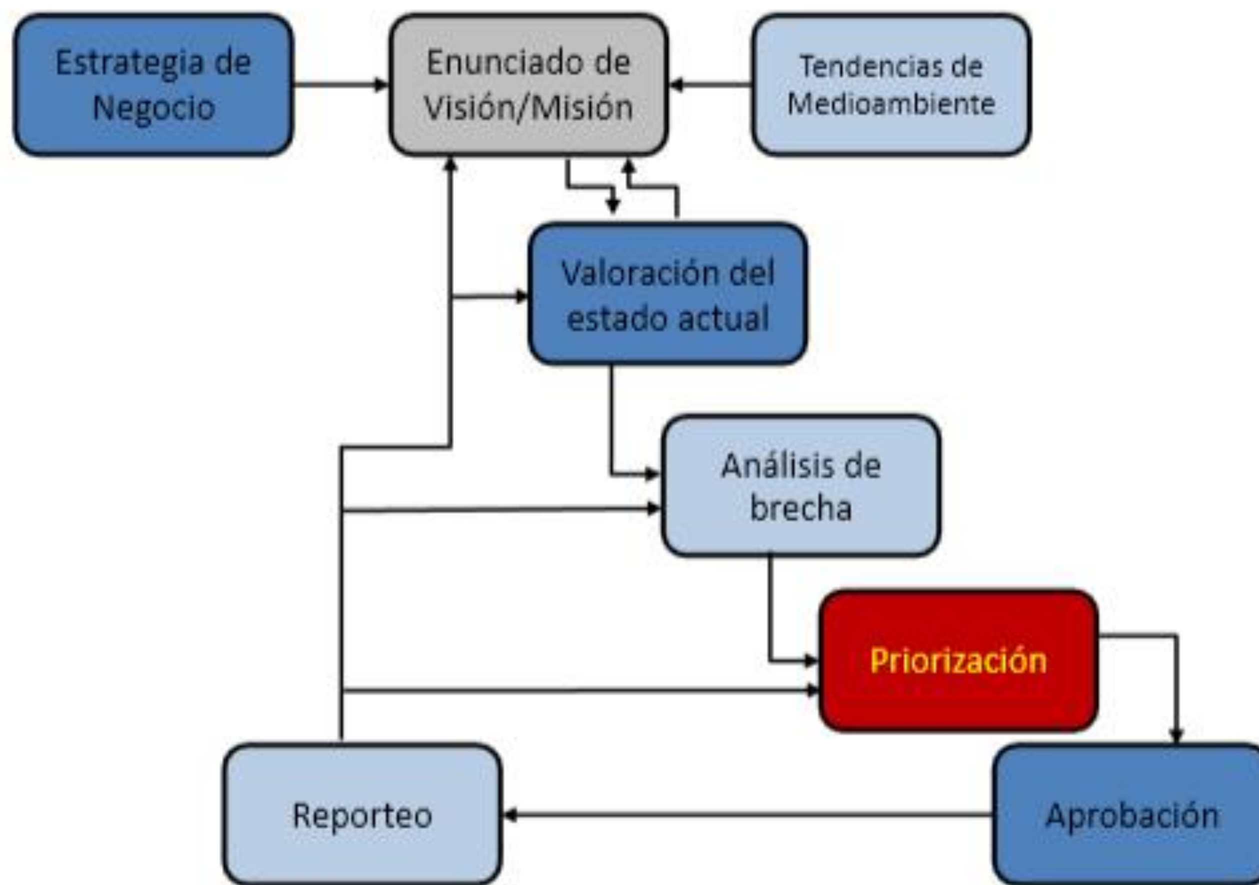
| Category | Future State | Current Situation | Action/Proposals |
|---|---|---|---|
| Identify | Centralized security governance to provide comprehensive risk management | Security is decentralized across business units | |
| Protect | Protect key system and processes used for drug, research, development, and trails | Security protections are not consistently applied | |
| Detect | Ability to quickly detect threats targeting intellectual property | Inability to detect malicious or negligent activity | |
| Respond | Ability to minimize data loss, block attacks, and determine root cause | Inability to mitigate attacks and limit the amount of data lost | |
| Recover | Capability to quickly return to normal operations and limit business impact of security incidents | Recovery and business continuity is decentralized | |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Análisis de brecha

| Category | Future State | Current Situation | Action/Proposals |
|---|---|---|---|
| Identify | Centralized security governance to provide comprehensive risk management | Security is decentralized across business units | Name a permanent CISO<br>Develop central policy library<br>Implement vulnerability Management program |
| Protect | Protect key system and processes used for drug, research, development, and trails | Security protections are not consistently applied | Decrease patch deployment time<br>Protect clinical trial systems<br>Deploy systems in blocking mode |
| Detect | Ability to quickly detect threats targeting intellectual property | Inability to detect malicious or negligent activity | Deploy continuous monitoring & log management capability<br>Advanced analytics and reporting<br>Implement DLP to monitor IP loss |
| Respond | Ability to minimize data loss, block attacks, and determine root cause | Inability to mitigate attacks and limit the amount of data lost | Build and staff 24x7 SOC<br>Develop advanced forensics team<br>Create threat intelligence sharing capability |
| Recover | Capability to quickly return to normal operations and limit business impact of security incidents | Recovery and business continuity is decentralized | Develop business continuity plan<br>Ensure that response plan is regularly tested<br>Socialize and communicate with BU leaders |

# Proceso de la PEdC



# Creando la hoja de ruta

Un proceso de 3 etapas:

1️⃣ Identificar lo que se está haciendo hoy

2️⃣ Correlacionar las capacidades actuales con los niveles de madurez

3️⃣ Priorizar nuevas iniciativas para aumentar la madurez

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# 1. ID Capacidades Actuales

- Documentar las actividades actuales
  - Hay que darle crédito a lo que se ha hecho hoy día

- Ejemplos de la función "Proteger" del NIST CSF
  - VPN, firewall, segmentación de la red
  - Cifrado de endpoint, antivirus, antimalware
  - Web single sign-on (SSO)
  - Concientización de los empleados
  - Estándares de seguridad

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# 2. Mapear nivel madurez

| Function | Category | Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
|---|---|---|---|---|---|---|
| Protect | Access Control | VPN<br>firewall,<br>segmentation | Web SSO | Federated SSO | | |
| | Awareness & Training | Basic awareness training | Phishing exercises | | | |
| | Data Security | Encryption data at rest and in-transit | Data segregation<br>Asset destruction | | | |
| | Processes & Procedures | Security standards change control | Integration with HR processes<br>Incident response plan | Security Development Process | | |
| | Protective Technology | Network and host security | Web application security program | Mobile application security | | |

# 3. Priorizar iniciativas

Determinar que iniciativas deben priorizarse para cruzar la brecha

- El costo no debe ser el único factor
- Incorporar el valor para el negocio y la defensa de amenazas
- Tomar en cuenta la habilidad para ejecutar y el soporte organizacional

ISACA®

Confianza en, y valor de los sistemas de información

Monterrey Chapter

# Matriz análisis de decisiones

| Initiative | Cost | Ability to Execute | Stakeholder Support | Threat Defense | Total |
|---|---|---|---|---|---|
| Mobile & BYOD | 3 | 5 | 5 | 4 | 17 |
| DLP | 2 | 3 | 4 | 5 | 14 |
| Centralized Vulnerability Management | 2 | 4 | 3 | 5 | 14 |
| Risk-Based Authentication | 3 | 3 | 4 | 3 | 13 |
| Network Access Control | 1 | 2 | 2 | 4 | 9 |

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Hoja de ruta – Proteger NIST

| Function | Category | Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
|---|---|---|---|---|---|---|
| Protect | Access Control | VPN<br>firewall,<br>segmentation | Web SSO | Federated SSO | Risk-based Authentication | Network Access Control |
| | Awareness & Training | Basic awareness training | Phishing exercises | Role-based training | Executive education | Third-party training program |
| | Data Security | Encryption data at rest and in-transit | Data segregation<br>Asset destruction | DLP (email & host) | DLP (cloud data storage) | Self protecting data |
| | Processes & Procedures | Security standards change control | Integration with HR processes<br>Incident response plan | Security Development Process | Centralized vulnerability management | Continuous feedback with business processes |
| | Protective Technology | Network and host security | Web application security program | Mobile application security | BYOD security | Cloud security program |

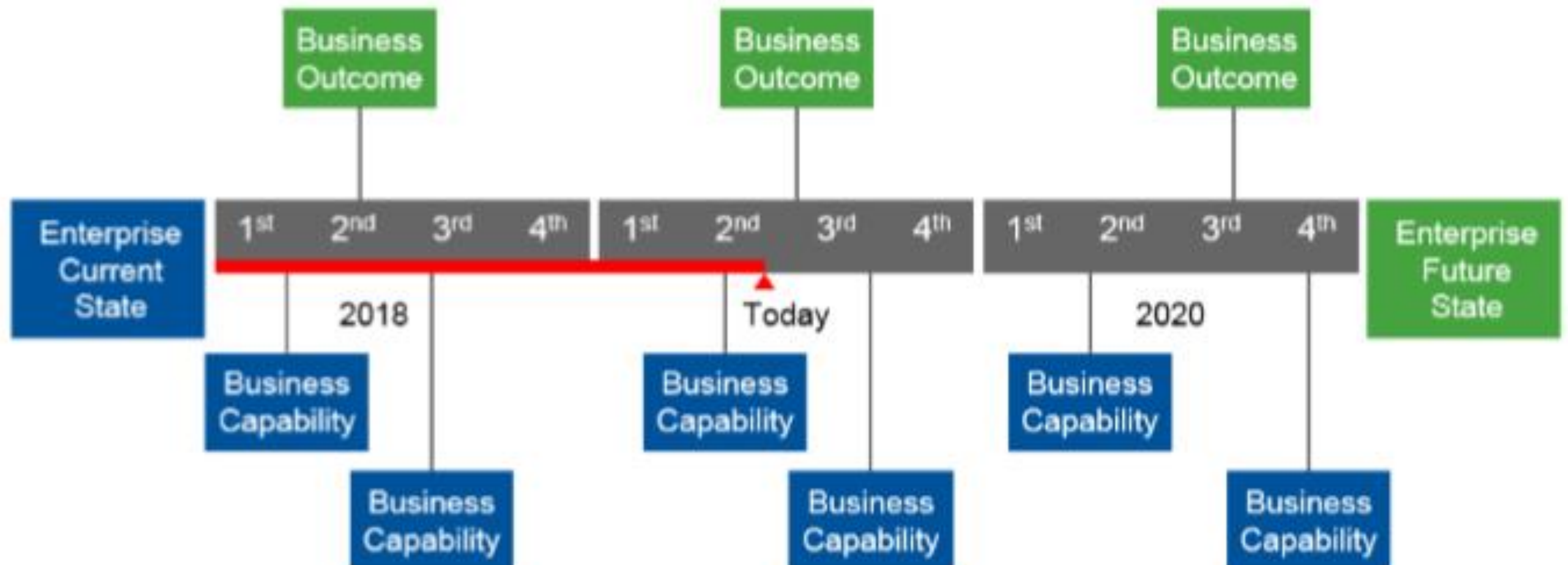
Done today

Started Doing

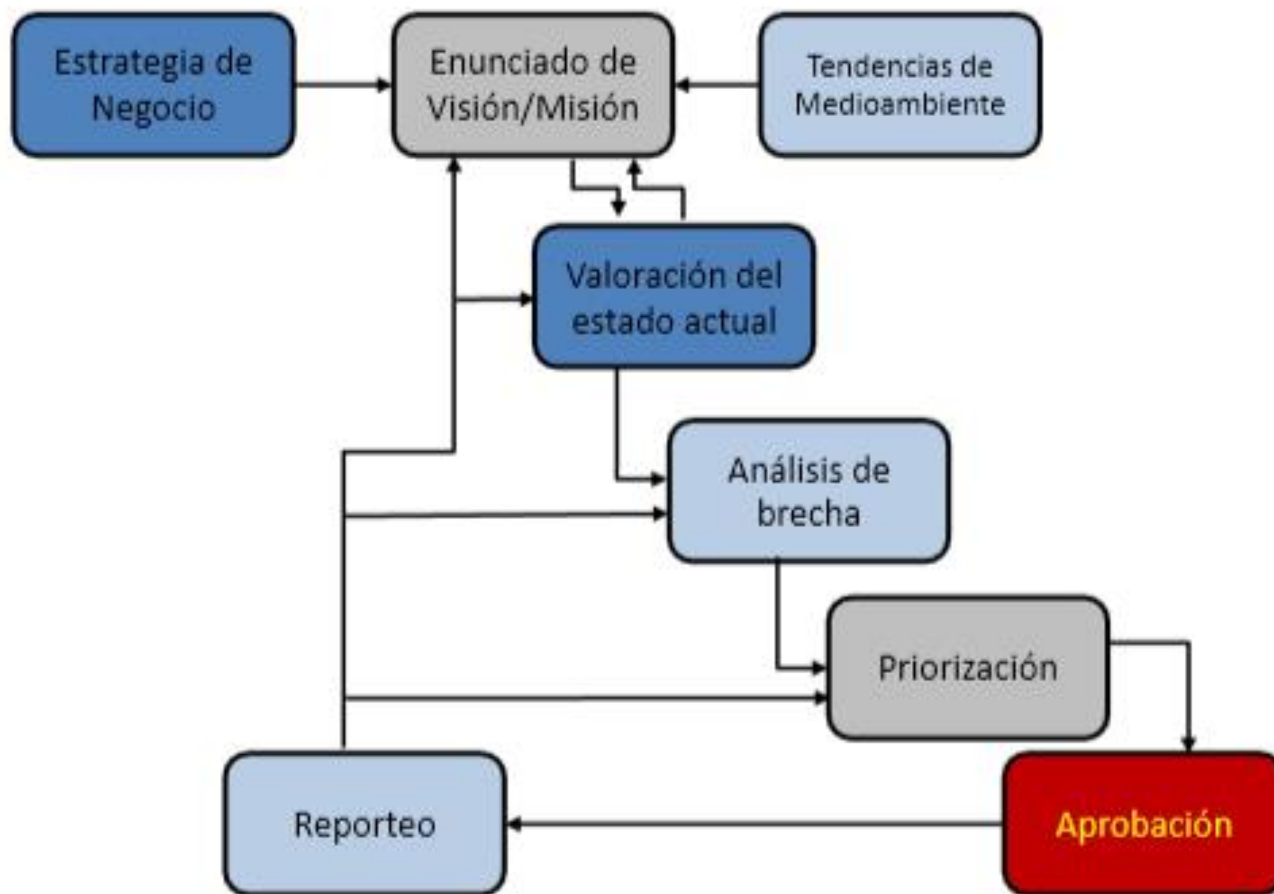
Start Immediate

Plan to start

# La hoja de ruta ejecutiva



# Proceso de la PEdC



# Algunas trampas

- “Si no lo hacemos nos van a hackear” (FUD)
- “Es la manera correcta de hacerlo”
- “Esta tecnología resolverá todos nuestros problemas”
- “No cuesta tanto”
- “La dirección no lo entiende”

# Caso de Negocio

- Captura la razón para iniciar el esfuerzo
- Estima de manera clara los costos y beneficios
- Da un análisis y descripción detallada de la iniciativa




# Enfoques casos de negocio

- Costo
- Comparación de la industria
- Innovación de negocios

# Enfoque innovación

Planear las inversiones de seguridad basadas en:

- Oportunidades de negocio
- Requerimientos de negocio
- Riesgo de negocio

ISACA

Confianza en, y valor de los sistemas de información

Monterrey Chapter

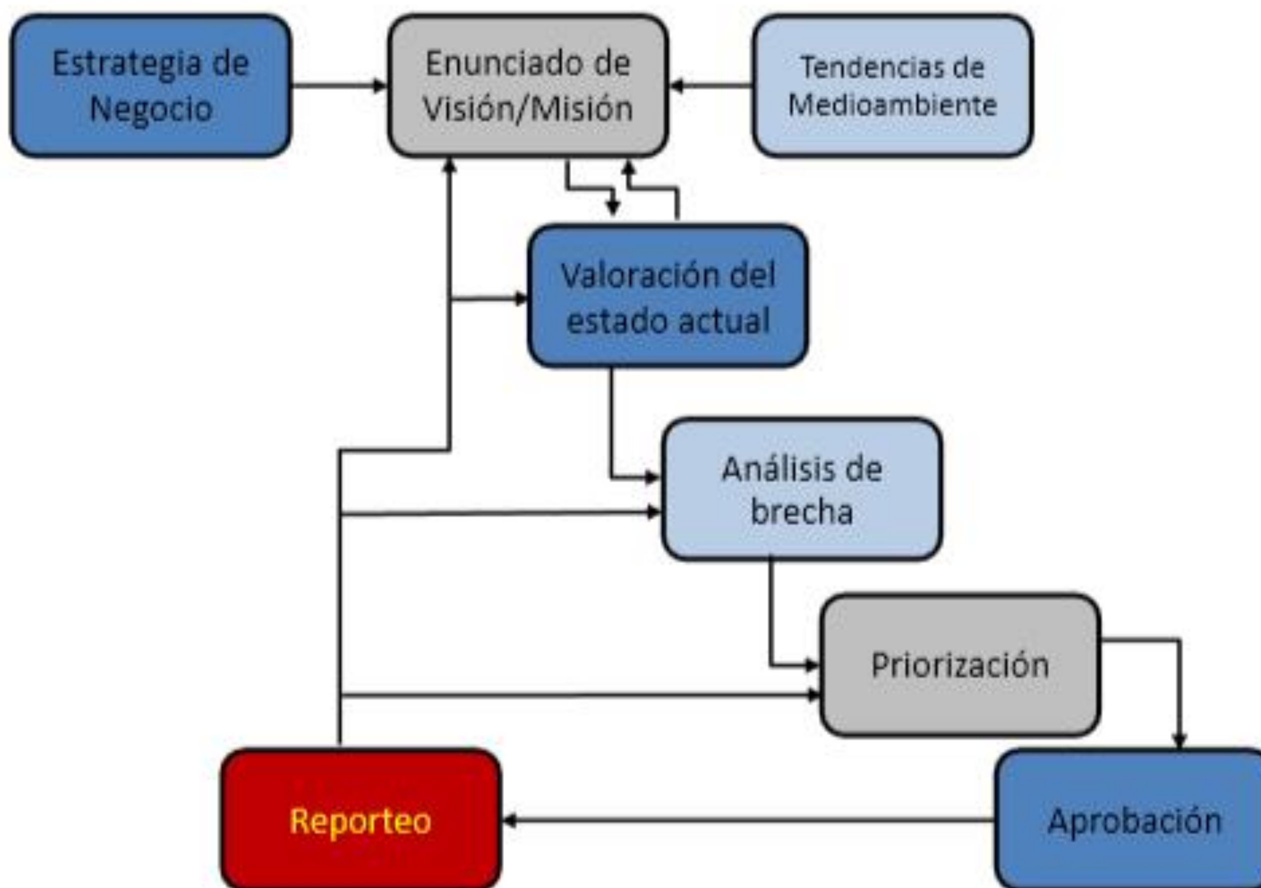
# Elementos caso de negocio

- Resumen ejecutivo
  - Problema
  - Valoración
  - Recomendaciones
- Introducción
  - Factores que impulsan al negocio
  - Alcances
  - Financiamiento
- Análisis
  - Suposiciones
  - Costo/beneficio
  - Riesgos clave
  - Dependencias y sinergias
  - Opciones
- Apéndice

Confianza en, y valor de los sistemas de información

Monterrey Chapter

# Proceso de la PEdC



# Importancia de las métricas

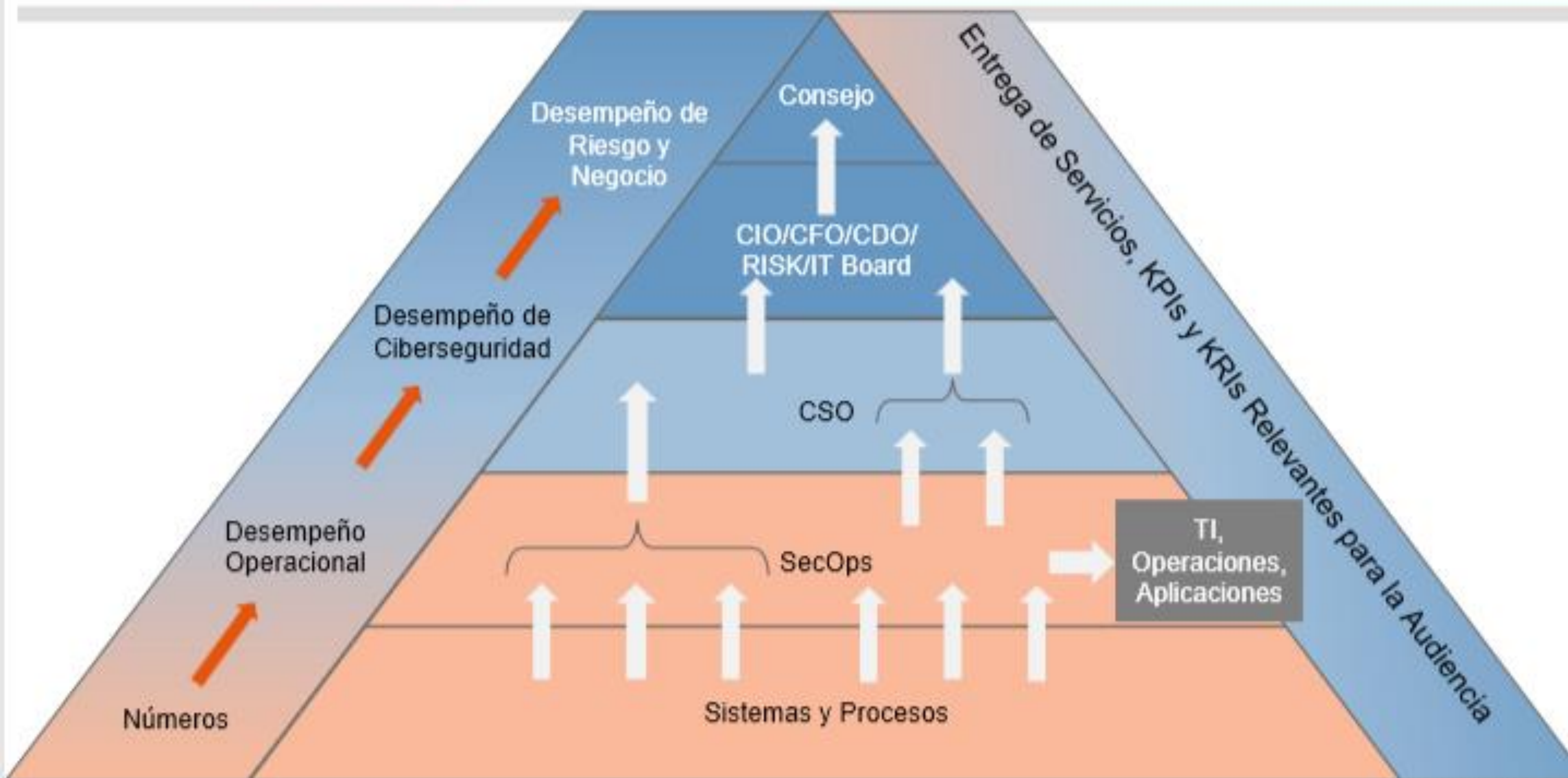
- Problema
  Muchos ejecutivos están buscando estadísticas de seguridad que sean importantes, de tal manera que sepan cuando y a qué poner atención
- Solución
  Proveer métricas esenciales que transformen y comuniquen información complicada en lenguaje de negocio que sea fácilmente entendible

# Importancia de las métricas

- Informar
- Educar
- Impulsar cambios de comportamiento

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Jerarquía de reporteo



# El abismo de las métricas

| CISO tradicional | | CIO | | El Negocio |
|---|---|---|---|---|

| Riesgo Tecnológico | Sistemas Tecnológicos | Procesos de Negocio | Objetivo de Negocio |
|---|---|---|---|
| Credenciales comprometidas | Robo de propiedad intelectual | Pérdida de momentum del mercado | Baja en Ingresos |

Las métricas técnicas llegan hasta aquí

Nadie cruza esta brecha

Las líneas de negocio ven hasta aquí

# Retos en métricas de seguridad

- Foco en **métricas técnicas**
- Uso de **listas genéricas** de métricas
- La brecha entre lo que seguridad hace y los **beneficios para el negocio**
- El contexto técnico en el que son desarrolladas **no invitan al cambio**

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Dar contexto a las métricas

Número de servidores escaneados/Sin escanear
Número de parches críticos e importantes

Convertir a porcentaje permite la normalización y crea tendencias



Porcentaje de parches críticos e importantes faltantes
Porcentaje de fallas en escaneo de servidores

Añadir contexto de negocio provee enlace con el negocio



Porcentaje de servidores críticos para el negocio y bases de datos mantenidas con cumplimiento de parches al 100%

Enfocarse en un sistema de negocio incrementa la relevancia para las partes interesadas



Porcentaje de parches críticos faltantes en facturación
Porcentaje de incremento de escaneos fallidos en facturación

Crear un enlace entre el indicador de riesgo y el proceso de negocio



Porcentaje de facturación tardía debido a caídas no programadas

Se completa el enlace con el impacto al negocio

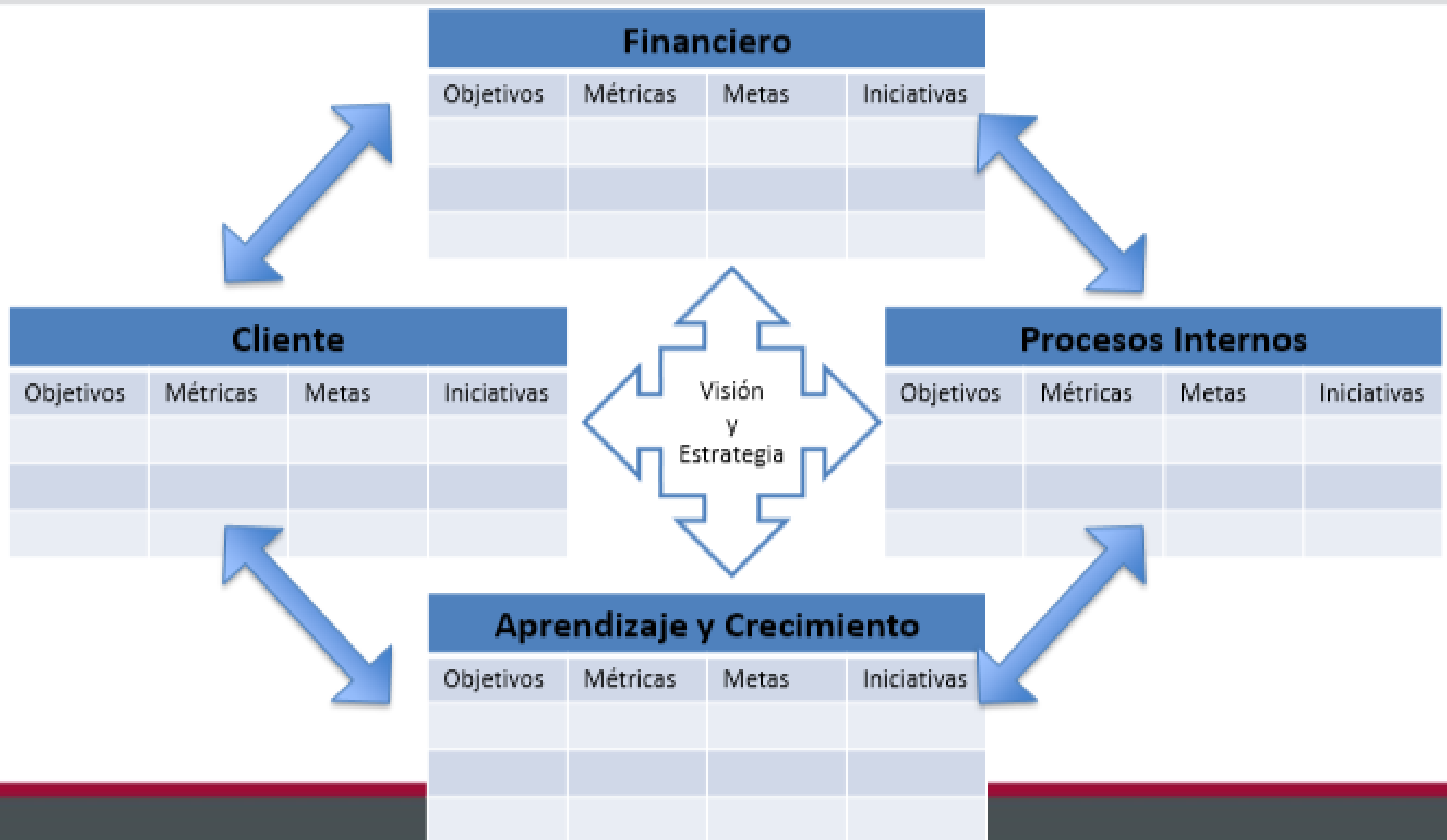




Facturación tardía causada por caídas no programadas que ponen la operación del negocio en riesgo

ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Balanced Scorecard



ISACA®
Confianza en, y valor de los sistemas de información
Monterrey Chapter

# Balanced Scorecard

## Enterprise XYZ — Balanced Scorecard for Information Security

**Balanced Score Card (Security) — Summary**

| Financial | 93% | R | Customer | 98% | A |
|---|---|---|---|---|---|
| F1 We will use security to help grow the business. | | A | C1 We will provide a high level of service availability and continuity. | | G |
| F2 We will be efficient in our security management. | | G | C2 Customers will have confidence in our services and facilities. | | G |
| F3 We will execute projects on time and on budget. | | G | C3 We will comply with all applicable regulations. | | A |
| F4 We will manage our suppliers cost-effectively. | | R | C4 The right people will have access to the right information — no more, no less. | | A |

| Operational | 90% | R | Learning and Growth | 95% | R |
|---|---|---|---|---|---|
| O1 Our tools will be fit for purpose. | | A | G1 Our people will be fully engaged. | | G |
| O2 We will execute change efficiently and reliably. | | G | G2 Our people will make the right decisions. | | G |
| O3 We will embed continuous improvement in our processes. | | A | G3 We will invest in our people and develop their expertise. | | A |
| O4 We will maintain our operational risk to within a defined risk appetite. | | R | G4 We will protect our know-how as a competitive advantage. | | R |


“Lo importante no es la meta
sino el camino recorrido”



¡GRACIAS!

David Hernández
davidhdz@protectia.com.mx

www.protectia.com.mx